

日 本 国 特 許 庁
JAPAN PATENT OFFICE

A. Shin
Filed 7/10/03
Q 76456
10f1

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 7月10日

出 願 番 号

Application Number:

特願2002-200920

[ST.10/C]:

[JP2002-200920]

出 願 人

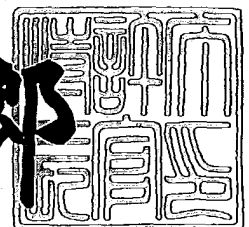
Applicant(s):

日本電気株式会社

2003年 5月 6日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田 信一郎



出証番号 出証特2003-3032903

【書類名】 特許願

【整理番号】 56200013PY

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/28
H04L 12/56
H04L 12/46

【発明者】

【住所又は居所】 東京都港区芝五丁目7番1号 日本電気株式会社内

【氏名】 進 昭宏

【特許出願人】

【識別番号】 000004237

【氏名又は名称】 日本電気株式会社

【代理人】

【識別番号】 100083987

【弁理士】

【氏名又は名称】 山内 梅雄

【手数料の表示】

【予納台帳番号】 016252

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9006535

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ユーザ認証システムおよびユーザ認証方法

【特許請求の範囲】

【請求項1】 通信端末と、

この通信端末から認証を要する所定の通信ネットワークに対して送り出されたパケット信号をその手前で入力するパケット信号入力手段と、このパケット信号入力手段が入力したパケット信号が前記所定の通信ネットワークに認証を受けたものであるか否かを判別する認証有無判別手段と、この認証有無判別手段が未認証と判別したときこれを出力する未認証ポートと、前記認証有無判別手段が認証済と判別したときこれを出力する認証済ポートとを備えた物理ポート切替手段と、

この物理ポート切替手段の未認証ポートから前記パケット信号が出力されたとき、そのパケット信号を送出した通信端末に対してログイン用の一時使用IPアドレスを一時的に与える一時使用アドレス提供手段と、

この一時使用アドレス提供手段の提供した一時使用IPアドレスと通信端末の対応関係を記憶する一時使用IPアドレス通信端末対応記憶手段と、

前記一時使用アドレス提供手段によって一時使用IPアドレスの提供を受けた通信端末が前記所定の通信ネットワークに対して認証を受けるためにログインしそのパケット信号が前記未認証ポートから出力されたときこれを入力してログイン画面を表示するログイン画面表示手段と、

このログイン画面表示手段を使用して前記通信端末からログインが行われたときこれに対して認証を行うか否かを判別する認証可否判別手段と、

この認証可否判別手段が認証を行うと判別したとき前記一時使用IPアドレス通信端末対応記憶手段に記憶された通信端末に対応させる形でこれに対して一時使用IPアドレスに代えて認証の対象となった所望の通信ネットワークに転送するためのネットワークアドレスを与えるネットワークアドレス付与手段とを具備することを特徴とするユーザ認証システム。

【請求項2】 前記ネットワークアドレス付与手段によってネットワークアドレスを付与された前記通信端末がパケット信号を送出したときこれを前記認証

済ポートを経て受信し、これを該当する通信ネットワークに振り分けるネットワーク振り分け手段を具備することを特徴とする請求項1記載のユーザ認証システム。

【請求項3】 通信端末と、

この通信端末から認証を要する所定の通信ネットワークに対して送り出されたパケット信号をその手前で入力するパケット信号入力手段と、このパケット信号入力手段が入力したパケット信号が前記所定の通信ネットワークに認証を受けたものであるか否かを判別する認証有無判別手段と、この認証有無判別手段が未認証と判別したときこれを出力する未認証ポートと、前記認証有無判別手段が認証済と判別したときこれを出力する認証済ポートとを備えた物理ポート切替手段と、

この物理ポート切替手段の未認証ポートから前記パケット信号が出力されたとき、そのパケット信号を送出した通信端末に対してログイン用の一時使用IPアドレスを一時的に与える一時使用アドレス提供手段と、

この一時使用アドレス提供手段の提供した一時使用IPアドレスと通信端末の対応関係を記憶する一時使用IPアドレス通信端末対応記憶手段と、

前記一時使用アドレス提供手段によって一時使用IPアドレスの提供を受けた通信端末が前記所定の通信ネットワークに対して認証を受けるためにログインしそのパケット信号が前記未認証ポートから出力されたときこれを入力してログイン画面を表示するログイン画面表示手段と、

このログイン画面表示手段を使用して前記通信端末からログインが行われたときこれに対して認証を行うか否かを判別する認証可否判別手段と、

この認証可否判別手段が認証を行うと判別したとき前記一時使用IPアドレス通信端末対応記憶手段に記憶された通信端末に対応させる形でこれに対して一時使用IPアドレスに代えて正規のIPアドレスを与える正規IPアドレス付与手段

とを具備することを特徴とするユーザ認証システム。

【請求項4】 前記正規IPアドレス付与手段によってIPアドレスを付与された前記通信端末がパケット信号を送出したときこれを前記認証済ポートを経

て受信し、これを該当するIPネットワークに振り分けるIPサブネット振り分け手段を具備することを特徴とする請求項3記載のユーザ認証システム。

【請求項5】 前記認証有無判別手段は認証を受けているユーザを登録したユーザ登録部を備え、このユーザ登録部に登録されているか否かによってユーザごとに認証が行われているか否かを判別することを特徴とする請求項1または請求項3記載のユーザ認証システム。

【請求項6】 前記IPサブネット振り分け手段は、IPアドレスと前記通信端末のMACアドレスのいずれかを用いて通信端末から送られてきたパケット信号の振り分けを行うことを特徴とする請求項4記載のユーザ認証システム。

【請求項7】 通信端末と、

この通信端末からアクセスがあったときこれに対してインターネットでアクセス可能なアドレスを与えるアドレス付与手段と、

このアドレス付与手段によって付与されたアドレスを使用して前記通信端末が認証を要求したとき、インターネットアクセス時に表示されるウェブ表示画面を認証用画面として認証のための入力操作および表示を行わせる認証時ウェブアクセス手段

とを具備することを特徴とするユーザ認証システム。

【請求項8】 前記IPサブネット振り分け手段は、前記IPアドレスとMACアドレスの双方が一致した宛先の通信ネットワークにパケット信号を振り分けることを特徴とする請求項4記載のユーザ認証システム。

【請求項9】 インターネットへのアクセスを行うに際してローカルエリアネットワークに接続されたネットワークサービスプロバイダに対して所定の通信端末からパケット信号を送出しインターネットへのアクセス要求を行うインターネットアクセス要求ステップと、

このインターネットアクセス要求ステップでインターネットへのアクセス要求があったときこの通信端末に対してログイン用の一時使用IPアドレスを返送する一時使用IPアドレス返送ステップと、

この一時使用IPアドレス返送ステップで返送されてきた一時使用IPアドレスを使用して前記通信端末から特定のインターネットサービスプロバイダに対す

る認証要求の packets 信号を送出する認証要求ステップと、

この認証要求ステップで送られてきた packets 信号に記された情報を基にして前記特定のインターネットサービスプロバイダの認証が得られるか否かをネットワークサービスプロバイダ側で判別する認証可否判別ステップと、

この認証可否判別ステップで認証が得られると判別したときその通信端末に対して前記特定のインターネットサービスプロバイダ用に割り当てられた IP アドレスを返送する正規 IP アドレス返送ステップと、

この正規 IP アドレス返送ステップで返送されてきた正規 IP アドレスを使用して前記通信端末からインターネットアクセス用の packets 信号を送出するインターネットアクセス用 packets 信号送出ステップと、

このインターネットアクセス用 packets 信号送出ステップで送出された packets 信号を受信しその前記正規 IP アドレスを見てこれを前記特定のインターネットサービスプロバイダに振り分ける packets 信号振り分けステップとを具備することを特徴とするユーザ認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、たとえば複数のローカルエリアネットワークのいずれかを選択的に使用するユーザや、ADSL 通信技術を使用して packets 信号を特定のインターネットサービスプロバイダを経由してインターネットに送出するユーザが、これらのネットワークに認証を行って接続するのに好適なユーザ認証システムおよびユーザ認証方法に関する。

【0002】

【従来の技術】

通信設備の整備拡張に伴って、ADSL (Asymmetric Digital Subscriber Line) 等の xDSL (x Digital Subscriber Line) 通信技術を使用して常時接続の環境でインターネットにアクセスすることが多くなっている。

【0003】

図6は、ADSLを使用してネットワークサービスプロバイダに接続する従来

の通信システムの概要を表わしたものである。この通信システム100で、パーソナルコンピュータからなる通信端末101はモデム（変復調装置）102を介してブロードバンドアクセスサーバ（BAS：Broadband Access Server）103と接続されている。ブロードバンドアクセスサーバ103は、ADSL等のxDSLあるいはFTTH（Fiber To The Home）等の高速なインターネット常時接続サービスを提供するために、図示しない通信局舎内に設置されるサーバをいう。ブロードバンドアクセスサーバ103は、通常の場合、複数のインターネットサービスプロバイダ（ISP：Internet Service Provider）104₁、104₂、……を介して図示しないインターネット網に接続されている。

【0004】

このような通信システム100では、ポイントツーポイントプロトコル・オーバ・イーサネット（登録商標）（PPP over E：Point To Point Protocol over Ethernet（登録商標））セッション105を使用して、通信端末101からブロードバンドアクセスサーバ103までポイントツーポイントデータを転送するようにしている。ここでこのポイントツーポイント・オーバ・イーサネット（登録商標）プロトコルは2点間を接続してデータ通信を行うためのプロトコルである。このプロトコルを使用することでTCP/IP（Transmission Control Protocol/Internet Protocol）を始めとする多くのプロトコルを中継することができる。ここでは、イーサネット（登録商標）等のローカルエリアネットワークで、IPアドレスを組み込んだパケット信号をカプセル化してブロードバンドアクセスサーバ103に転送するためにポイントツーポイントプロトコルセッション105が使用される。たとえば特開平10-173691号公報にこの種の技術が開示されている。

【0005】

ブロードバンドアクセスサーバ103はローカルエリアネットワーク上を通信端末101から送られてきた信号をデカプセル化してパケット信号を取り出し、通信端末101が契約したインターネットサービスプロバイダ104_xにこれを転送する。インターネットサービスプロバイダ104_xは通信端末101に対してパスワードを要求する等の手法で本人確認としての認証を行い、これが成功し

たら通信端末101から送られてきたパケット信号をそのIPアドレスの示す相手先に送出することになる。

【0006】

このように、この図6に示した通信システム100では、通信端末101がインターネットサービスプロバイダ104_xに直接接続されていれば本来必要としないポイントツーポイントプロトコルを使用してパケット信号をカプセル化して転送している。このためブロードバンドアクセスサーバ103はポイントツーポイントプロトコルによるヘッダの取り付けや取り外しといったパケット信号のカプセル化やデカプセル化の作業を必要とする。現在、インターネットへの常時接続の環境が急速に整ってきており、これに伴って加入者端末101がその契約した特定のインターネットサービスプロバイダ104_xを通して通信するパケット信号の量が増加している。また、常時接続に適したアプリケーションソフトウェアの登場やウェブサイトの増加によって、今後、ますます加入者端末101とインターネットサービスプロバイダ104_xの間の通信量が増加することは確実である。このような状況の下では、ポイントツーポイントプロトコルを使用したパケット信号のカプセル化あるいはカプセルを取り除くデカプセル化の作業を撤廃あるいは軽減する必要がある。

【0007】

図7は、以上説明したポイントツーポイントプロトコルを使用しないで済む従来提案された通信システムの概要を表わしたものである。この図7で図6と同一部分には同一の符号を付しており、これらの説明を適宜省略する。この通信システム120では、通信端末101がVLAN (Virtual Local Area Network) スイッチ121に接続されている。VLANスイッチ121は、バーチャル・ローカルエリアネットワーク122₁、122₂、……によって複数のインターネットサービスプロバイダ (ISP: Internet Service Provider) 104₁、104₂、……を介して図示しないインターネット網に接続されている。したがって、通信端末101がインターネットサービスプロバイダ104_xとインターネットの接続について契約を行っているものとする、VLANスイッチ121は通信端末101がログインすると認証を行い、認証が成功すれば契約先のインターネッ

トサービスプロバイダ 1 0 4_xと接続する。なお、VLANについては特開平 0 9 - 1 3 0 4 2 1 号公報等に掲載がある。

【0008】

【発明が解決しようとする課題】

この図 7 に示した通信システム 1 2 0 では、図 6 で説明したようなポイントツーポイントプロトコルを使用する必要がない。したがって、プロトコルスタック数が多すぎるためにブロードバンド化という観点から、既存の設備としてのブロードバンドアクセスサーバ 1 0 3 やルータがボトルネックとなるという問題から開放される。また、認証が終わった後にはバーチャルなローカルエリアネットワークとしてのバーチャル・ローカルエリアネットワーク 1 2 2₁、1 2 2₂、……に接続されるので、スループットの点で大幅な改善が期待される。

【0009】

しかしながら、この通信システム 1 2 0 ではバーチャル・ローカルエリアネットワークを採用している。このため、VLANスイッチ 1 2 1 が分岐できるバーチャル・ローカルエリアネットワークの数は、バーチャル・ローカルエリアネットワークを転送されるフレームのVLANフィールドが 1 2 ビット構成となっていることから、2 の 1 2 乗個、すなわち 4 0 9 6 個が最大となっている。ローカルエリアネットワークはたとえば 1 つの企業内でも部署や物理的な位置に応じて多数組まれる場合があり、これらを集合して更に大きなネットワークを構成していったとき、この制限は通信システムの構築に大きな制約となる。

【0010】

そこで本発明の目的は、通信端末がローカルエリアネットワークを介して自在に通信ネットワークや所望のローカルエリアネットワークに数の制約なく接続することのできるユーザ認証システムおよびユーザ認証方法を提供することにある。

【0011】

【課題を解決するための手段】

請求項 1 記載の発明では、（イ）通信端末と、（ロ）この通信端末から認証を要する所定の通信ネットワークに対して送り出されたパケット信号をその手前で

入力するパケット信号入力手段と、このパケット信号入力手段が入力したパケット信号が前記した所定の通信ネットワークに認証を受けたものであるか否かを判別する認証有無判別手段と、この認証有無判別手段が未認証と判別したときこれを出力する未認証ポートと、認証有無判別手段が認証済と判別したときこれを出力する認証済ポートとを備えた物理ポート切替手段と、（ハ）この物理ポート切替手段の未認証ポートからパケット信号が出力されたとき、そのパケット信号を送出した通信端末に対してログイン用の一時使用 I P アドレスを一時的に与える一時使用アドレス提供手段と、（ニ）この一時使用アドレス提供手段の提供した一時使用 I P アドレスと通信端末の対応関係を記憶する一時使用 I P アドレス通信端末対応記憶手段と、（ホ）一時使用アドレス提供手段によって一時使用 I P アドレスの提供を受けた通信端末が前記した所定の通信ネットワークに対して認証を受けるためにログインしそのパケット信号が未認証ポートから出力されたときこれを入力してログイン画面を表示するログイン画面表示手段と、（ヘ）このログイン画面表示手段を使用して通信端末からログインが行われたときこれに対して認証を行うか否かを判別する認証可否判別手段と、（ト）この認証可否判別手段が認証を行うと判別したとき一時使用 I P アドレス通信端末対応記憶手段に記憶された通信端末に対応させる形でこれに対して一時使用 I P アドレスに代えて認証の対象となった所望の通信ネットワークに転送するためのネットワークアドレスを与えるネットワークアドレス付与手段とをユーザ認証システムに具備させる。

【 0 0 1 2 】

すなわち請求項 1 記載の発明では、通信端末が送出したパケット信号を、認証を要する所定の通信ネットワークの手前に配置された物理ポート切替手段が入力するようになっている。そして、これが認証済であるかどうかを判別し、認証済でない場合にはそのパケット信号を送出した通信端末に対してログイン用の一時使用 I P アドレスを一時的に与えるようにしている。一時使用 I P アドレスを受け取った通信端末は、これを用いてパケット信号を送出し物理ポート切替手段の未認証ポートを経てログイン画面表示手段に入力され、ログイン画面の表示が行われる。通信端末はログイン画面で認証のためのログインを行い、認証可否判別

手段が認証を行うか否かを判別する。認証が成功した場合には一時使用 IP アドレスに代えて認証の対象となった所望の通信ネットワークに転送するためのネットワークアドレスが与えられる。したがって、それ以後は物理ポート切替手段の認証済ポートを介して所望の通信ネットワークとの通信が可能になる。ネットワークアドレスの数は前記した VLAN フィールドのビット数による制限がないので、通信システムの構築の自由度が拡大する。また、ネットワークアドレスによってパケット信号の宛先を処理するので、ポイントツーポイントプロトコルを使用した技術と比較して処理が単純化し、スループットが低下することはない。

【0013】

請求項 2 記載の発明では、請求項 1 記載のユーザ認証システムは、ネットワークアドレス付与手段によってネットワークアドレスを付与された通信端末がパケット信号を送出したときこれを認証済ポートを経て受信し、これを該当する通信ネットワークに振り分けるネットワーク振り分け手段を具備することを特徴としている。

【0014】

すなわち請求項 2 記載の発明では、ネットワーク振り分け手段がネットワークアドレスによって通信端末が送出したパケット信号の振り分けを行うことにしている。

【0015】

請求項 3 記載の発明では、（イ）通信端末と、（ロ）この通信端末から認証を要する所定の通信ネットワークに対して送り出されたパケット信号をその手前で入力するパケット信号入力手段と、このパケット信号入力手段が入力したパケット信号が前記した所定の通信ネットワークに認証を受けたものであるか否かを判別する認証有無判別手段と、この認証有無判別手段が未認証と判別したときこれを出力する未認証ポートと、認証有無判別手段が認証済と判別したときこれを出力する認証済ポートとを備えた物理ポート切替手段と、（ハ）この物理ポート切替手段の未認証ポートからパケット信号が出力されたとき、そのパケット信号を送出した通信端末に対してログイン用の一時使用 IP アドレスを一時的に与える一時使用アドレス提供手段と、（ニ）この一時使用アドレス提供手段の提供した

一時使用 IP アドレスと通信端末の対応関係を記憶する一時使用 IP アドレス通信端末対応記憶手段と、（ホ）一時使用アドレス提供手段によって一時使用 IP アドレスの提供を受けた通信端末が前記した所定の通信ネットワークに対して認証を受けるためにログインしそのパケット信号が未認証ポートから出力されたときこれを入力してログイン画面を表示するログイン画面表示手段と、（ヘ）このログイン画面表示手段を使用して通信端末からログインが行われたときこれに対して認証を行うか否かを判別する認証可否判別手段と、（ト）この認証可否判別手段が認証を行うと判別したとき一時使用 IP アドレス通信端末対応記憶手段に記憶された通信端末に対応させる形でこれに対して一時使用 IP アドレスに代えて正規の IP アドレスを与える正規 IP アドレス付与手段とをユーザ認証システムに具備させる。

【0016】

すなわち請求項3記載の発明では、通信端末が送出したパケット信号を、認証を要する所定の通信ネットワークの手前に配置された物理ポート切替手段が入力するようになっている。そして、これが認証済であるかどうかを判別し、認証済でない場合にはそのパケット信号を送出した通信端末に対してログイン用の一時使用 IP アドレスを一時的に与えるようにしている。一時使用 IP アドレスを受け取った通信端末は、これを用いてパケット信号を送出し物理ポート切替手段の未認証ポートを経てログイン画面表示手段に入力され、ログイン画面の表示が行われる。通信端末はログイン画面で認証のためのログインを行い、認証可否判別手段が認証を行うか否かを判別する。認証が成功した場合には一時使用 IP アドレスに代えて認証の対象となった所望の通信ネットワークに転送するための正規の IP アドレスが与えられる。したがって、それ以後は物理ポート切替手段の認証済ポートを介して所望の通信ネットワークとの通信が可能になる。IP アドレスによって特定される宛先の数は無制限に近い数まで可能であり、前記した VLAN フィールドのビット数による制限がないので、通信システムの構築の自由度が拡大する。また、IP アドレスによってパケット信号の宛先を処理するので、ポイントツーポイントプロトコルを使用した技術と比較して処理が単純化し、スループットが低下することはない。

【0017】

請求項4記載の発明では、請求項3記載のユーザ認証システムは、正規IPアドレス付与手段によってIPアドレスを付与された通信端末がパケット信号を送出したときこれを認証済ポートを経て受信し、これを該当するIPネットワークに振り分けるIPサブネット振り分け手段を具備することを特徴としている。

【0018】

すなわち請求項4記載の発明では、IPサブネット振り分け手段がIPパケットのサブネットアドレスによって通信端末が送出したパケット信号の振り分けを行うことにしている。

【0019】

請求項5記載の発明では、請求項3記載のユーザ認証システムで、認証有無判別手段は認証を受けているユーザを登録したユーザ登録部を備え、このユーザ登録部に登録されているか否かによってユーザごとに認証が行われているか否かを判別することを特徴としている。

【0020】

すなわち請求項5記載の発明では、認証前のパケット信号について認証を行う必要があるので認証有無判別手段でユーザ登録部を用いてその判別を行うようにしている。ユーザ登録部は認証されているユーザを登録しておりこれを検索することで認証の有無を判別することができる。ユーザの特定は、たとえばMACアドレスを用いて行うことができる。

【0021】

請求項6記載の発明では、請求項4記載のユーザ認証システムで、IPサブネット振り分け手段は、IPアドレスと通信端末のMACアドレスのいずれかを用いて通信端末から送られてきたパケット信号の振り分けを行うことを特徴としている。

【0022】

すなわち請求項6記載の発明では、IPサブネット振り分け手段の振り分けの態様を規定している。IPアドレスを振り分け先の通信ネットワークにそれぞれ対応付けて用意しておけば、IPアドレスを調べるだけでどの通信ネットワーク

に振り分けるかを判別することができる。これ以外に通信端末のMACアドレスを用いて振り分けを行うことも可能である。このように振り分けについて2種類の情報を使い分けることで、パケット信号の振り分けを、個々のユーザに与えるIPアドレスによってあるいはハードウェア自体によって異なった観点から行うことができる。

【0023】

請求項7記載の発明では、(イ)通信端末と、(ロ)この通信端末からアクセスがあったときこれに対してインターネットでアクセス可能なアドレスを与えるアドレス付与手段と、(ハ)このアドレス付与手段によって付与されたアドレスを使用して通信端末が認証を要求したとき、インターネットアクセス時に表示されるウェブ表示画面を認証用画面として認証のための入力操作および表示を行わせる認証時ウェブアクセス手段とをユーザ認証システムに具備させる。

【0024】

すなわち請求項7記載の発明では、アドレス付与手段が通信端末からアクセスがあったときこれに対してインターネットでアクセス可能なアドレスを、とりあえず与えることにしている。そして、この通信端末が与えられたアドレスを用いて認証を要求してきたときには、認証時ウェブアクセス手段がインターネットアクセス時に表示されるウェブ表示画面を認証用画面として認証のための入力操作および表示を行わせることにしている。このようにウェブ表示画面を用いて認証の手続きを行うので、通信端末に特別な認証用のアプリケーションソフトウェアをインストールすることなく、通常備わっているブラウザを使用して認証のための操作が可能である。

【0025】

請求項8記載の発明では、請求項4記載のユーザ認証システムで、IPサブネット振り分け手段は、IPアドレスとMACアドレスの双方が一致した宛先の通信ネットワークにパケット信号を振り分けることを特徴としている。

【0026】

すなわち請求項8記載の発明では、請求項4記載のユーザ認証システムで、IPサブネット振り分け手段は、IPアドレスとMACアドレスの双方が一致した

場合を扱っている。このように両者が一致する場合で振り分け先を決めることでセキュリティを高めることが可能になる。

【0027】

請求項9記載の発明では、（イ）インターネットへのアクセスを行うに際してローカルエリアネットワークに接続されたネットワークサービスプロバイダに対して所定の通信端末からパケット信号を送出しインターネットへのアクセス要求を行うインターネットアクセス要求ステップと、（ロ）このインターネットアクセス要求ステップでインターネットへのアクセス要求があったときこの通信端末に対してログイン用の一時使用IPアドレスを返送する一時使用IPアドレス返送ステップと、（ハ）この一時使用IPアドレス返送ステップで返送されてきた一時使用IPアドレスを使用して通信端末から特定のインターネットサービスプロバイダに対する認証要求のパケット信号を送出する認証要求ステップと、（ニ）この認証要求ステップで送られてきたパケット信号に記された情報を基にして前記した特定のインターネットサービスプロバイダの認証が得られるか否かをネットワークサービスプロバイダ側で判別する認証可否判別ステップと、（ホ）この認証可否判別ステップで認証が得られると判別したときその通信端末に対して前記した特定のインターネットサービスプロバイダ用に割り当てられたIPアドレスを返送する正規IPアドレス返送ステップと、（ヘ）この正規IPアドレス返送ステップで返送されてきた正規IPアドレスを使用して通信端末からインターネットアクセス用のパケット信号を送出するインターネットアクセス用パケット信号送出ステップと、（ト）このインターネットアクセス用パケット信号送出ステップで送出されたパケット信号を受信しその正規IPアドレスを見てこれを前記した特定のインターネットサービスプロバイダに振り分けるパケット信号振り分けステップとをユーザ認証方法に具備させる。

【0028】

すなわち請求項9記載の発明では、インターネットへのアクセスを行うのに際してローカルエリアネットワークに接続されたネットワークサービスプロバイダに対して所定の通信端末からパケット信号を送出し、インターネットへのアクセス要求を行い、ネットワークサービスプロバイダ側からログイン用の一時使用IP

Pアドレスを返送してもらう。そして、この一時使用IPアドレスを使用して通信端末から特定のインターネットサービスプロバイダに対する認証要求の packets 信号を送出して（認証要求ステップ）、この packets 信号に記された情報を基にして前記した特定のインターネットサービスプロバイダの認証が得られるか否かをネットワークサービスプロバイダ側で判別させる（認証可否判別ステップ）。この認証可否判別ステップで認証が得られると判別されたときには、その通信端末に対してネットワークサービスプロバイダ側から前記した特定のインターネットサービスプロバイダ用に割り当てられたIPアドレスが正規アドレスとして返送される（正規IPアドレス返送ステップ）。この場合には、この正規IPアドレスを使用して通信端末からインターネットアクセス用の packets 信号がネットワークサービスプロバイダ側に送出されると（インターネットアクセス用 packets 信号送出ステップ）、ネットワークサービスプロバイダ側ではこの packets 信号の正規IPアドレスを見てこれを前記した特定のインターネットサービスプロバイダ側に振り分けることができる（packets 信号振り分けステップ）。したがって、それ以後は所望の通信ネットワークとの通信が可能になる。IPアドレスの数は前記したVLANフィールドのビット数による制限がないので、通信システムの構築の自由度が拡大する。また、IPアドレスによって packets 信号の宛先を処理するので、ポイントツーポイントプロトコルを使用した技術と比較して処理が単純化し、スループットが低下することはない。

【0029】

【発明の実施の形態】

【0030】

【実施例】

以下実施例につき本発明を詳細に説明する。

【0031】

<第1の実施例>

【0032】

図1は本発明の第1の実施例におけるユーザ認証システムを表わしたものである。このユーザ認証システム200で、加入者端末201はイーサネット（登録

商標) (Ethernet (登録商標)) 等のネットワーク (以下、ローカルエリアネットワークと称する。) 202と接続されている。このローカルエリアネットワーク202は、ネットワークサービスプロバイダ (NSP: Network Service Provider) 203内に位置する物理ポートの切り替えを行う物理ポート切替スイッチ204の入力側と接続されている。物理ポート切替スイッチ204は認証済の物理ポートに対応する認証ポート205と、認証が行われていない物理ポートに対応する未認証ポート206の2つのポートの切り替えを行うスイッチである。認証ポート205は、ユーザの認証が行われた後のIPパケットを転送する認証IPネットワーク207に接続されている。

【0033】

認証IPネットワーク207は、本実施例の場合、IPパケットをサブネットによって第1のインターネットサービスプロバイダ (ISP: Internet Service Provider) 208₁あるいは第2のインターネットサービスプロバイダ208₂のうちの一方の経路に振り分けて送信するIPサブネット振分スイッチ209に接続されている。IPアドレスはネットワークアドレスとホストアドレスの2つに分けられるが、そのうち、ネットワークアドレスをさらに分割したものがサブネットワークアドレスである。IPサブネット振分スイッチ209は、IPアドレスにおけるサブネットワークアドレスを見て、第1のターゲットIPネットワーク214₁のネットワークアドレスと一致していれば、加入者端末201から送出されたフレーム信号を、第1のターゲットIPネットワーク214₁にフォワード (転送) する。これに対して、第2のターゲットIPネットワーク214₂のネットワークアドレスと一致していれば、このフレーム信号を第2のターゲットIPネットワーク214₂にフォワードすることになる。

【0034】

また、認証IPネットワーク207は、加入者端末201の認証を行うための認証IPネットワークDHCPサーバ211の一端と接続されている。ここで、DHCP (Dynamic Host Configuration Protocol) とは、各ユーザに、起動時に動的にIPアドレスを割り当て、終了時にこのIPアドレスを回収するためのプロトコルである。認証IPネットワークDHCPサーバ211は、物理ポート

切替スイッチ204から送られてきた送信元のMACアドレスを第1および第2のRADIUS (Remote Authentication Dialin User Service) サーバ213₁、213₂のうちの該当するもの、すなわち認証の対象となるインターネットサービスプロバイダ208を担当する者に渡してIPアドレスを受け取り、これを加入者端末201に割り当てる役割をもっている。第1および第2のRADIUSサーバ213₁、213₂のうち該当するものは、クライアントからのダイヤルアップ接続認証要求を受けて、認証の可否をクライアントに返すようになっている。認証IPネットワークDHCPサーバ211の他端は、このユーザ認証システム200でユーザの認証のための管理に使用される管理用IPネットワーク212と接続されている。

【0035】

一方、物理ポート切替スイッチ204の未認証ポート206側には、未認証の packets 信号を入力して認証のための処理を行うためのデフォルトIPネットワーク217が接続されている。このデフォルトIPネットワーク217には、未認証の packets 信号をログインさせるためのログイン用ウェブサーバ215とデフォルトIPネットワーク用DHCP (Dynamic Host Configuration Protocol) サーバ216のそれぞれ一端が接続されている。ここで、ログイン用ウェブサーバ215は、特別なソフトウェアをインストール必要なく、一般にパーソナルコンピュータの購入時等に付属している使用料が不要あるいは安価なウェブページ閲覧用のソフトウェアを使用してログインさせるためのものである。デフォルトIPネットワーク用DHCPサーバ216は、再利用可能なIPアドレスの動的割り当てを行うためのサーバであり、具体的にはログイン用ウェブサーバ215でログインを行わせるために臨時にIPアドレスを与えるサーバである。これらログイン用ウェブサーバ215およびデフォルトDHCPサーバ216は管理用IPネットワーク212とも接続されている。

【0036】

管理用IPネットワーク212は、前記した認証IPネットワークDHCPサーバ211と接続している他に、第1および第2のRADIUSサーバ213₁、213₂とも接続している。これらRADIUSサーバ213₁、213₂は、

加入者端末201からのダイヤルアップ接続認証要求を受けて、認証の可否をクライアントに返す役割を持っている。また、第1のRADIUSサーバ213₁は、加入者端末201が第1のターゲットIPネットワーク214₁および第1のインターネットサービスプロバイダ208₁を経てインターネット網に接続するものであれば、このような振分けを可能とするIPアドレスをこれに与えるようになっている。これに対して、加入者端末201が第2のターゲットIPネットワーク214₂および第2のインターネットサービスプロバイダ208₂を経てインターネット網に接続するものである場合には、このような振分けを可能とするIPアドレスをこれに与えることになる。

【0037】

ところで本実施例のユーザ認証システム200で物理ポート切替スイッチ204はローカルエリアネットワーク202を経てネットワークサービスプロバイダ203に加入者端末201側から送られてきたパケット信号を受信する。そしてそのパケット信号の送信元のMAC(Media Access Control)アドレスを調べ、これに応じてポートの切替制御を行うようになっている。

【0038】

図2は、この物理ポート切替スイッチの制御の様子を表わしたものである。図1に示した物理ポート切替スイッチ204は、図示しないがCPU(中央処理装置)、制御プログラムを格納する記憶媒体、出力ポートを切り替える切替手段ならびにMACアドレスを登録するMACアドレス登録テーブルを備えている。物理ポート切替スイッチ204はパケット信号が到来すると(ステップS301:Y)、そのMACアドレスを判別する(ステップS302)。MACアドレスは、NIC(Network Interface Card)ごとに割り当てられる番号であり、6オクテットで表わされている。そしてこのMACアドレスと同一のアドレスがMACアドレス登録テーブルに登録されているか検索する(ステップS303)。

【0039】

本実施例のMACアドレス登録テーブルには、ユーザ認証を受けたMACアドレスを登録するようにしている。ただし、一度登録を行ったMACアドレスであってもログアウトした時点でその登録内容は消去されるようになっている。物理

ポート切替スイッチ204内の前記したCPUは受信したパケット信号のMACアドレスがMACアドレス登録テーブルに登録されているものであれば（ステップS304：Y）、物理ポートを認証ポート205側に切り替えて（ステップS305）、そのパケット信号を図1に示す認証IPネットワーク207へ送り出す。

【0040】

これに対して、受信したパケット信号のMACアドレスがMACアドレス登録テーブルに登録されていない場合には（ステップS304：N）、物理ポートを未認証ポート206側に切り替えて（ステップS306）、そのパケット信号を図1に示すデフォルトIPネットワーク217へ送り出すことになる。

【0041】

今、図1に示した加入者端末201のユーザが第1のインターネットサービスプロバイダ208₁とインターネット網の接続について契約を行っているものとする。このユーザが、インターネットにアクセスするために所定の時点で加入者端末201のブラウザを立ち上げて第1のインターネットサービスプロバイダ208₁に対する認証要求のための処理を開始したものとする。これにより加入者端末201から送出されたパケット信号は、第1のインターネットサービスプロバイダ208₁の手前に配置されたネットワークサービスプロバイダ203の物理ポート切替スイッチ204に入力される。物理ポート切替スイッチ204はこの認証がまだ行われていない時点で加入者端末201のMACアドレスをMACアドレス登録テーブルに登録していない。そこで、ユーザ認証を行うためのユーザのログインを可能とする仮のIPアドレスを与える手続きに入ることになる。

【0042】

図3は、本実施例のユーザ認証システムの原理的な構成を示したものである。ユーザ認証システム200の主要部を構成するネットワークサービスプロバイダ203は、ローカルエリアネットワーク202を通じてパケット信号401を物理ポート切替スイッチ204に入力する。このとき、まだ所定のインターネットサービスプロバイダ208との間でインターネットの接続を行うための認証が行われていないので、物理ポート切替スイッチ204はユーザ認証手段402と接

続し、ユーザ認証の手続きを開始する。この手続きでユーザ認証が成功すると、ネットワークサービスプロバイダ203はその加入者端末201にIPアドレスを与える。このときIPサブネットアドレス払出手段403はネットワークサービスプロバイダ203側が予め貯蔵しておいたIPアドレスの中から1つをその加入者端末201用に払い出す。これについては後に具体的に説明する。

【0043】

この後、加入者端末201が送出したパケット信号には、ネットワークサービスプロバイダ203側でその払い出されたIPアドレスが使用される。これにより、物理ポート切替スイッチ204から認証IPネットワーク207へ送り出されたパケット信号は、後に詳細を説明するIPアドレスMACアドレスフィルタ手段404に入力されてフィルタリングされ、振分手段405でIPサブネットワークを見て特定のインターネットサービスプロバイダ208あるいは図示しない通信ネットワークに振り分けられることになる。ユーザの振分けとしてのフィルタリングはIPアドレスによって行うこともMACアドレスによって行うことも可能である。両者の組み合わせによってもよい。

【0044】

さて、以上の概略の説明の後に、再びユーザ認証手段402の処理の箇所から具体的な説明を行う。ユーザがインターネットに接続するために加入者端末201を操作すると、加入者端末201からIPアドレスを取得するためにDHCPリクエストパケットが送出される。

【0045】

図4は、DHCPリクエストパケットが送出された時点以降の本実施例のユーザ認証システムにおける加入者端末側の処理の概要を表わしたものである。図1と共にこれを説明する。加入者端末201はDHCPリクエストパケットをブロードキャストフレームで送信する（ステップS501）。物理ポート切替スイッチ204はこれを受信すると未認証ポート206に接続されたデフォルトIPネットワーク217にフォワードする。

【0046】

デフォルトIPネットワーク217に収容されているデフォルトIPネットワ

ーク用DHCPサーバ216は、加入者端末201から送られてきたDHCPリクエストパケットを受け取る。そして、受け取ったことを示す“ack”信号を返送する。したがって、加入者端末201はこの“ack”信号を受信するまで（ステップS502：N）、DHCPリクエストパケットの送出を繰り返すことになる。

【0047】

デフォルトIPネットワーク用DHCPサーバ216はこの“ack”信号を返送するが、このとき加入者端末201に対して予め用意した未使用のIPアドレスを付加して送信する。この結果として、加入者端末201はDHCPリクエストパケットの受信を意味する“ack”信号を受信したら（ステップS502：Y）、次に臨時に割り当てられたこのIPアドレスを取得することになる（ステップS503）。この臨時のIPアドレスを割り当てたとき、デフォルトIPネットワーク用DHCPサーバ216は、加入者端末201のMACアドレスと、このMACアドレスに割り当てたIPアドレスをその図示しない記憶領域に記憶しておく。また、このとき割り当てるIPアドレスは有限な時間でリースされるものであるため、リース時間tを設定する。一例としては、リース時間tを5秒程度に設定する。もちろん、リース時間tは1時間といったように、これより長い時間であってもよい。

【0048】

このようにしてIPアドレスが一時的に割り当てられると、加入者端末201はそのウェブ（WEB）ブラウザを用いてログイン用ウェブサーバ215にアクセスする。ログイン用ウェブサーバ215は、“http”（hypertext transfer protocol）手順でユーザIDとパワーを入力するために必要とされる画面情報を加入者端末201に送信する。ここで“http”手順とは、HTML（Hyper Text Markup Language）転送のためのハイパーテキスト転送プロトコルとして規定された要求と返答を組み合わせた手順をいう。画面情報の送信によって、加入者端末201は認証のためのユーザIDとパワーを入力する画面を表示することができる。

【0049】

この画面の表示状態で加入者は加入者端末201を操作して、ユーザIDとパスワードを“http”手順で入力する。ログイン用ウェブサーバ215は“http”手順でアクセスしてきた加入者端末201のIPアドレスを管理用IPネットワーク212を経由してデフォルトIPネットワーク用DHCPサーバ216に渡す。デフォルトIPネットワーク用DHCPサーバ216は加入者端末201のIPアドレスを受け取ると、そのIPアドレスに対応する加入者端末201のMACアドレスをログイン用ウェブサーバ215に通知する。ログイン用ウェブサーバ215は加入者端末201のMACアドレスの通知を受けると、これと先に受け取ったユーザIDおよびパスワードを、管理用IPネットワーク212を経由して第1および第2のRADIUSサーバ213₁、213₂のうち該当するものへ渡して認証の依頼を行う。

【0050】

今、加入者端末201がインターネットの接続について契約を行っている第1のインターネットサービスプロバイダ208₁に関しては、第1のRADIUSサーバ213₁がこれを担当することになる。なお、第2のRADIUSサーバ213₂は第1のRADIUSサーバ213₁と基本的に同一の構成となっているため、その動作についての説明は省略する。

【0051】

この例の場合、第1のRADIUSサーバ213₁は、ログイン用ウェブサーバ215から受け取ったユーザIDとパスワードを認証する。そしてその結果をログイン用ウェブサーバ215に通知する。このとき、第1のRADIUSサーバ213₁はユーザIDとMACアドレスとを図示しない記憶領域に記憶しておく。

【0052】

ログイン用ウェブサーバ215は、第1のRADIUSサーバ213₁から認証結果を受け取る。パスワードが一致しない等の理由で認証が失敗であれば、ログイン用ウェブサーバ215はその旨を示す画面を“http”手順で加入者端末201に送り込む。認証が成功であれば、成功であることを示す画面を同様に“http”手順で加入者端末201に送り込む。また、認証が成功の場合、ロ

ゲイン用ウェブサーバ215は物理ポート切替スイッチ204に対して、今後この加入者端末201のMACアドレスを有するパケット信号を受け取った場合にはこれを認証ポート205と接続された認証IPネットワーク207にフォワードするように指示を送出する。

【0053】

この指示を受けた物理ポート切替スイッチ204は、前記したMACアドレス登録テーブルにそのMACアドレスを登録する。そして、加入者端末201がログアウトしない限り、同一のMACアドレスを持ったパケット信号が到来したとき、認証ポート205に接続された認証IPネットワーク207にフォワードするように動作することになる。

【0054】

このようにして加入者端末201がこれ以後、ローカルエリアネットワーク202に送出するパケット信号は物理ポート切替スイッチ204を介して認証IPネットワーク207にフォワードされるが、IPアドレスのリース時間は有限である。そこで、加入者端末201はリース時間 t の2分の1の時間が経過すると（ステップS504）、リースの延長を求めるDHCPリクエストパケットを送出する（ステップS505）。このDHCPリクエストパケットはユニキャストフレームとして送信される。臨時のIPアドレスが発行されたこの時点ではデフォルトIPネットワーク用DHCPサーバ216を宛先として送出される。

【0055】

このDHCPリクエストに対して、該当するデフォルトIPネットワーク用DHCPサーバ216から“ack”信号が返却されてきたときには（ステップS506：Y）、そのデフォルトIPネットワーク用DHCPサーバ216はその時点でリース時間 t を再延長している。したがって、加入者端末201はリース時間 t の2分の1の時間が経過するたびに同じ動作を繰り返すようにすることでリース時間 t を何回でも延長することができる。このようなリース時間 t が設けられている主旨は、加入者端末201がログアウトをしても同一のIPアドレスを保持する事態を避けて、予め用意したIPアドレスが枯渇することを防止するためである。

【0056】

ところで、加入者端末201がステップS505でリースの延長を求めるDHCPリクエストパケットを送出したにも係わらず該当するデフォルトIPネットワーク用DHCPサーバ216が何らかの原因で“ack”信号を返送しない場合がある(ステップS506:N)。このような場合には、リース時間tの8分の7の時間が経過する前までは(ステップS507:Y)、ステップS505に戻ってユニキャストフレームでDHCPリクエストパケットを繰り返し送出する。

【0057】

このようにDHCPリクエストパケットを繰り返し送出しても、該当するデフォルトIPネットワーク用DHCPサーバ216から“ack”信号が送り返されない場合には(ステップS507:N)、リース時間tの8分の7の時間に到達した時点で(ステップS507:N)、今度はブロードキャストフレームでDHCPリクエストパケットを送出する(ステップS508)。これにより、このDHCPリクエストはデフォルトIPネットワーク用DHCPサーバ216だけでなく認証IPネットワークDHCPサーバ211にも伝達されることになる。

【0058】

このDHCPリクエストに対して認証IPネットワークDHCPサーバ211から“ack”信号が送り返された場合には(ステップS509:Y)、リース時間tが更新される。これにより処理はステップS504に戻ることになる。これに対して“ack”信号が送り返されてこなかったような場合には(ステップS509:N)、リース時間tが切れるまで(ステップS510:N)、ブロードキャストフレームでDHCPリクエストパケットを繰り返し送出する(ステップS508)。そして、リース時間tが切れた時点で(ステップS510:Y)、そのIPアドレスを開放することになる(ステップS511)。

【0059】

ところで、認証IPネットワークDHCPサーバ211はDHCP手順によって加入者端末201のMACアドレスを知ることができる。そこで認証IPネットワークDHCPサーバ211は管理用IPネットワーク212を経由して担当

の第1のRADIUSサーバ213₁に加入者端末201のMACアドレスを渡して、これに対して割り当てるべき適切なIPアドレスを通知するように依頼する。

【0060】

第1のRADIUSサーバ213₁はこの依頼を受けると、認証IPネットワークDHCPサーバ211から加入者端末201のMACアドレスを受け取り、先に記憶しておいたユーザIDとMACアドレスの組み合わせから対応するユーザIDを取り出す。そしてこのユーザIDに割り当てるべきIPアドレスを決定し、認証IPネットワークDHCPサーバ211に対してこの決定したIPアドレスを通知する。なお、このIPアドレスは第1のRADIUSサーバ213₁が事前にストックしておいたアドレスの中から払い出すものであるが、これに限るものではない。たとえばデフォルトIPネットワーク用DHCPサーバ216が臨時で与えたIPアドレスをそのまま与えても差し支えない。ただし、デフォルトIPネットワーク用DHCPサーバ216が臨時で与えるIPアドレスは、ネットワークサービスプロバイダ203内で他のIPアドレスと競合するものでなければどのようなものでもよいが、第1のRADIUSサーバ213₁や第2のRADIUSサーバ213₂が払い出すIPアドレスはネットワークサービスプロバイダ203の外でも同一のものが無いことが条件となる。

【0061】

認証IPネットワークDHCPサーバ211は、割り当てるべきIPアドレスを、この例の場合、第1のRADIUSサーバ213₁から通知されると、加入者端末201からのDHCPリクエストパケットに対してIPアドレスを割り当てたことを通知する割当通知パケットを返送する。

【0062】

ところでIPサブネット振分スイッチ209は、認証IPネットワーク207からIPパケットが送られてくると、レイヤ3のIPサブネットワークアドレスをチェックして、それぞれ該当するIPネットワークへフォワードするようにこれらの対応関係をスタティックに設定している。その結果、たとえば第1のターゲットIPネットワーク214₁のサブネットワークに一致したサブネットワー

クアドレスのIPパケットが到来すればこれを第1のターゲットIPネットワーク214₁へフォワードする。また、第2のターゲットIPネットワーク214₂のサブネットワークに一致したサブネットワークアドレスのIPパケットが到来すればこれを第2のターゲットIPネットワーク214₂へフォワードすることになる。

【0063】

先の例では、加入者端末201がインターネット網へのアクセスについて第1のインターネットサービスプロバイダ208₁と契約している。したがって、第1のRADIUSサーバ213₁が加入者端末201用のIPアドレスを与えることになる。このIPアドレスのパケット信号はIPサブネット振分スイッチ209で第1のターゲットIPネットワーク214₁の第1のインターネットサービスプロバイダ208₁に送られ、これを經由して図示しないインターネット網に転送されることになる。

【0064】

<第2の実施例>

【0065】

図5は、本発明の第2の実施例におけるユーザ認証システムを表わしたものである。このユーザ認証システム600は、ある会社が社員や協力会社のスタッフのそれぞれにアクセスできるローカルエリアネットワークを振り分けるようにした認証システムである。ユーザ認証システム600は、パーソナルコンピュータからなる第1～第Nの入出力端末601₁～601_Nと、これらに共通して接続された社内一般向けローカルエリアネットワーク(LAN)602と、特殊目的あるいは用途の第1～第Mの専門別ローカルエリアネットワーク603₁～603_Mと、これら第1～第Mの専門別ローカルエリアネットワーク603₁～603_Mに対する認証と振分けを行う認証・振分け装置604とから構成されている。

【0066】

ここで、認証・振分け装置604は社内一般向けローカルエリアネットワーク602と接続された物理ポート切替スイッチ611を備えている。物理ポート切替スイッチ611は認証の行われたユーザの一覧を登録するユーザ登録テーブル

612を備えている。ユーザ登録テーブル612はユーザが第1～第Mの専門別ローカルエリアネットワーク603₁～603_Mのうちの特定のものにログインする要求を行って認証が成功したときに登録され、その専門別ローカルエリアネットワーク603からログアウトしたときに登録を消去されるようになっている。

【0067】

物理ポート切替スイッチ611はこのユーザ登録テーブル612の他に先の実施例と同様の未認証ポート613と認証ポート614を備えている。ユーザ登録テーブル612に登録されていないユーザからアクセスがあったときには未認証ポート613が選択され、送られてきたブロードキャストアドレスのパケットはこの未認証ポート613に接続された未認証用ネットワーク616に転送される。未認証用ネットワーク616には、ログイン用ウェブサーバ617とデフォルトアドレスサーバ618が接続されている。これらログイン用ウェブサーバ617とデフォルトアドレスサーバ618は管理用ネットワーク619にも接続されている。

【0068】

一方、認証ポート614には認証用ネットワーク621が接続されている。認証用ネットワーク621にはユーザが第1～第Mの専門別ローカルエリアネットワーク603₁～603_Mのうちのいずれか希望するものにログインするための認証を行う認証サーバ622と、アドレス振分スイッチ623が接続されている。アドレス振分スイッチ623はユーザから送られてきたパケット信号のサブアドレスに応じて第1～第Mの専門別ローカルエリアネットワーク603₁～603_Mのいずれかにこのパケット信号を振り分けて送出するようになっている。認証サーバ622は管理用ネットワーク619にも接続されている。また、管理用ネットワーク619にはこれ以外にサブアドレス付与サーバ624が接続されている。サブアドレス付与サーバ624は認証されたパケット信号のユーザに対して希望する専門別ローカルエリアネットワーク603に対応したサブアドレスを付与するようになっている。

【0069】

このようなユーザ認証システム600で、たとえば光ファイバの研究者である

ユーザAが社内の光ファイバに関する技術情報を集めた第1の専門別ローカルエリアネットワーク603₁にアクセスする場合を例にとって説明する。ユーザAは自己の社員証の磁気情報を第1～第Nの入出力端末601₁～601_Nのいずれかに接続された図示しない磁気情報読取装置から読み取らせる。この情報を組み込んだパケット信号は、認証・振分け装置604の物理ポート切替スイッチ611に入力される。

【0070】

物理ポート切替スイッチ611ではこのパケット信号に組み込まれた磁気カードの読取情報をキーとしてユーザ登録テーブル612を検索し、未認証であることを知る。そこで、このパケット信号は未認証ポート613から未認証用ネットワーク616に転送される。デフォルトアドレスサーバ618はこのパケット信号を受信するとこのユーザAに臨時で対応するIPアドレスを発行する。このIPアドレスはパケット信号の送信元のユーザAに返送される。ユーザAはこのIPアドレスを使用したパケット信号を認証要求のために送信し、ログイン用ウェブサーバ17によって一般的なブラウザによって認証用の画面が表示される。ユーザAはこの状態で、ログインする希望の第1の専門別ローカルエリアネットワーク603₁の名称と自己のパスワードを入力することになる。

【0071】

この入力情報は先の磁気情報と共に認証サーバ622に与えられる。認証サーバ622は第1～第Mの専門別ローカルエリアネットワーク603₁～603_Mのそれぞれに対する社員ごとのアクセス権限を記したテーブルを参照し、認証の可否を決定する。認証が成功したときにはサブアドレス付与サーバ624がユーザAの希望した第1の専門別ローカルエリアネットワーク603₁に対応したサブアドレスをユーザA用に設定する。このサブアドレスは認証成功の通知と共に社内一般向けローカルエリアネットワーク602を経てユーザAに返送される。また、認証が成功した時点でユーザ登録テーブル612にユーザAが登録される。

【0072】

この後、ユーザAが第1の専門別ローカルエリアネットワーク603₁に向けたパケット信号を送出すると、物理ポート切替スイッチ611はこれを認証ポー

ト 6 1 4 から認証用ネットワーク 6 2 1 に向けて送り出す。このパケット信号はアドレス振分スイッチ 6 2 3 に入力される。アドレス振分スイッチ 6 2 3 はパケット信号のサブアドレスを見て、このパケット信号を第 1 の専門別ローカルエリアネットワーク 6 0 3₁ に転送することになる。

【 0 0 7 3 】

なお、以上説明した第 1 の実施例では付与された IP アドレスのサブアドレスを用いてターゲット IP ネットワークを振り分ける処理を行ったが、そのパケット信号の MAC アドレスを併せて使用して、たとえば両者が一致する通信ネットワークに対してパケット信号の振り分けを行うことも可能である。これにより、IP アドレスを使用しただけの場合と比べて第三者が不用意に IP ネットワークに侵入する事態を回避し、セキュリティを向上させることができる。

【 0 0 7 4 】

また、第 1 の実施例では付与された IP アドレスのサブアドレスを用いてパケット信号の振り分けを行ったが、MAC アドレスのみで振り分けを行うことも可能である。

【 0 0 7 5 】

【発明の効果】

以上説明したように請求項 1 記載の発明によれば、通信端末が送出したパケット信号を、認証を要する所定の通信ネットワークの手前に配置された物理ポート切替手段が入力し、これが認証済でない場合にはそのパケット信号を送出した通信端末に対してログイン用の一時使用 IP アドレスを一時的に与えると共にログイン画面表示手段でログインの際の画面表示を行うようにした。これにより、通信端末にインターネット上の情報を表示するために一般的に備えられているブラウザを使用してログイン操作が可能になる。すなわち、ログインのために特別のソフトウェアを通信端末にインストールする必要がない。また、認証が成功した場合には一時使用 IP アドレスに代えて認証の対象となった所望の通信ネットワークに転送するためのネットワークアドレスが与えられるので、それ以後は物理ポート切替手段の認証済ポートを介して所望の通信ネットワークとの通信が可能になる。ネットワークアドレスの数は前記した VLAN フィールドのビット数に

よる制限がないので、通信システムの構築の自由度が拡大する。また、ネットワークアドレスによってパケット信号の宛先を処理するので、ポイントツーポイントプロトコルを使用した技術と比較して処理が単純化し、スループットが低下することはない。

【0076】

また、請求項2記載の発明によれば、ネットワーク振り分け手段を備えているので、通信端末が与えられたネットワークアドレスを使用することで単純にパケット信号の振り分けを行うことができる。

【0077】

更に請求項3記載の発明によれば、通信端末が送出したパケット信号を、認証を要する所定の通信ネットワークの手前に配置された物理ポート切替手段が入力し、これが認証済でない場合にはそのパケット信号を送出した通信端末に対してログイン用の一時使用IPアドレスを一時的に与えると共にログイン画面表示手段でログインの際の画面表示を行うようにした。これにより、通信端末にインターネット上の情報を表示するために一般的に備えられているブラウザを使用してログイン操作が可能になる。すなわち、ログインのために特別のソフトウェアを通信端末にインストールする必要がない。また、認証が成功した場合には一時使用IPアドレスに代えて正規のIPアドレスを与えるので、それ以後は物理ポート切替手段の認証済ポートを介して所望の通信ネットワークとの通信が可能になる。IPアドレスの数は前記したVLANフィールドのビット数による制限がないので、通信システムの構築の自由度が拡大する。また、ネットワークアドレスによってパケット信号の宛先を処理するので、ポイントツーポイントプロトコルを使用した技術と比較して処理が単純化し、スループットが低下することはない。

【0078】

また請求項4記載の発明によれば、IPサブネット振り分け手段を備えているので、通信端末が与えられたIPアドレスを使用することで単純にパケット信号の振り分けを行うことができる。

【0079】

更に請求項6記載の発明によれば、IPサブネット振り分け手段は、IPアドレスと通信端末のMACアドレスのいずれかを用いて通信端末から送られてきたパケット信号の振り分けを行うので、異なった観点からパケット信号の振り分けを行うことができる。

【0080】

また請求項7記載の発明によれば、通信端末からアクセスがあったときこれに対してインターネットでアクセス可能なアドレスを与えてウェブ表示画面を用いて認証の手続きを行うので、通信端末に特別な認証用のアプリケーションソフトウェアをインストールすることなく、通常備わっているブラウザを使用して認証のための操作が可能である。

【0081】

更に請求項8記載の発明によれば、IPサブネット振り分け手段は、IPアドレスとMACアドレスの双方が一致したことをもってパケット信号の振り分け先を決めることにしたので、アクセスに対するセキュリティを高めることが可能になる。

【0082】

また請求項9記載の発明によれば、一時使用IPアドレス返送ステップで一時使用IPアドレスを通信端末に返送し、これを使用して認証要求を行わせることにしたので、この一時使用IPアドレスを使用して認証のための手続きをインターネットサービスプロバイダの手前側で簡易に処理することができる。また、個々のインターネットサービスプロバイダ用にIPアドレスを振り分けておくことで、通信端末側から送られてきたパケット信号のIPアドレスを判読することでどのインターネットサービスプロバイダに振り分けるかを簡易に判別することができ、ポイントツーポイントプロトコルを使用した技術と比較して処理が単純化し、スループットが低下することはない。しかもIPアドレスの数は前記したVLANフィールドのビット数による制限がないので、通信システムの構築の自由度が拡大する。

【図面の簡単な説明】

【図1】

本発明の第1の実施例におけるユーザ認証システムを表わしたシステム構成図である。

【図2】

本実施例の物理ポート切替スイッチの制御の様子を表わした流れ図である。

【図3】

本実施例のユーザ認証システムにおける認証およびパケット信号の振り分けの原理を示した説明図である。

【図4】

DHCPリクエストパケットが送出された時点以降の本実施例のユーザ認証システムにおける加入者端末側の処理の概要を表わした流れ図である。

【図5】

本発明の第2の実施例におけるユーザ認証システムを表わしたシステム構成図である。

【図6】

ADSLを使用してネットワークサービスプロバイダに接続する従来の通信システムの概要を表わしたシステム構成図である。

【図7】

ポイントツーポイントプロトコルを使用しないで済む従来提案された通信システムの概要を表わしたシステム構成図である。

【符号の説明】

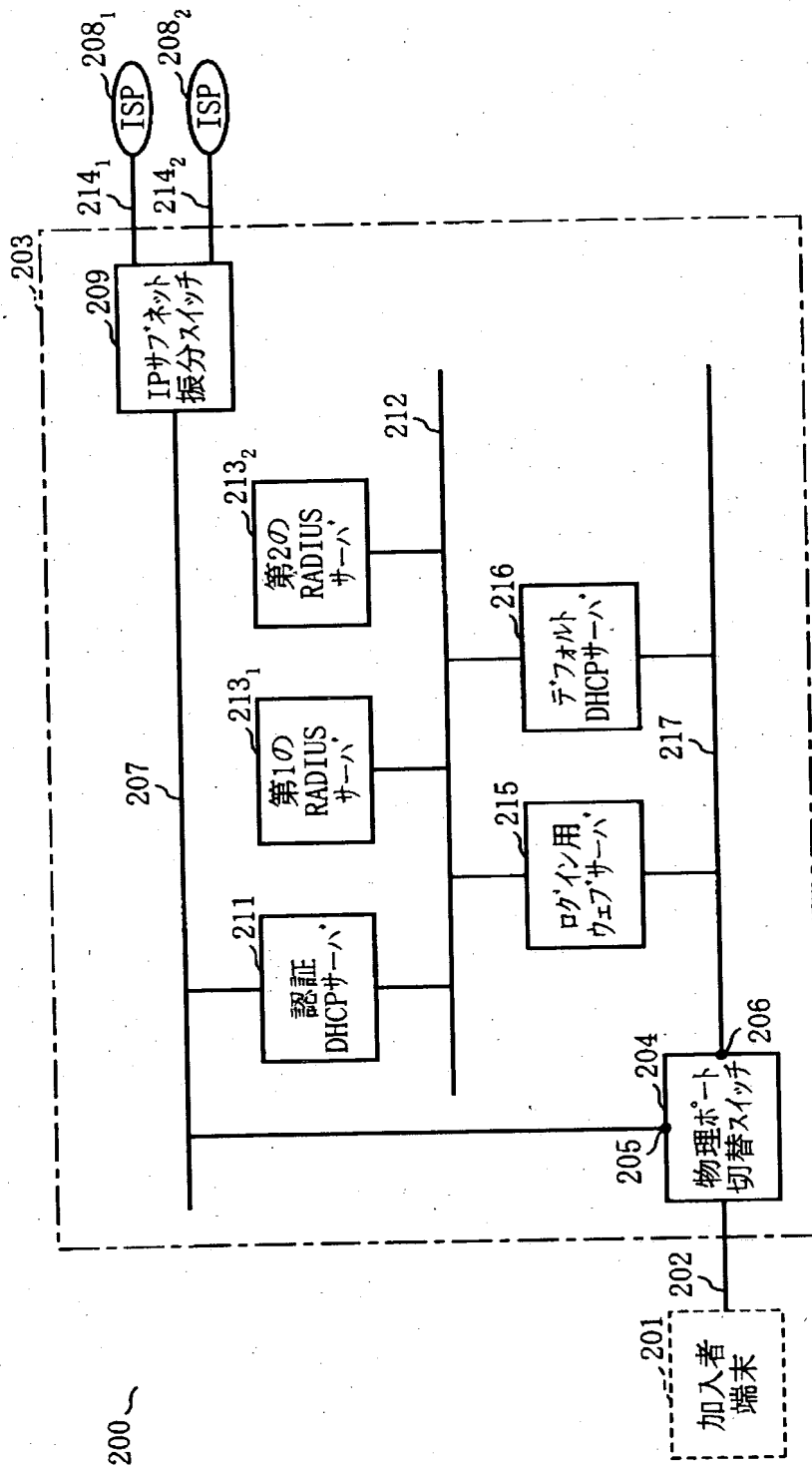
- 200、600 ユーザ認証システム
- 201 加入者端末
- 202 ローカルエリアネットワーク
- 204、611 物理ポート切替スイッチ
- 205 認証ポート
- 206 未認証ポート
- 207 認証IPネットワーク
- 209 IPサブネット振分スイッチ
- 211 認証IPネットワークDHCPサーバ

- 212 管理用IPネットワーク
- 213 RADIUSサーバ
- 214 ターゲットIPネットワーク
- 215、617 ログイン用ウェブサーバ
- 216 デフォルトIPネットワーク用DHCPサーバ
- 217 デフォルトIPネットワーク
- 401 パケット信号
- 402 ユーザ認証手段
- 403 IPサブネットアドレス払出手段
- 404 IPアドレスMACアドレスフィルタ手段
- 405 振分手段
- 601 入出力端末
- 602 社内一般向けローカルエリアネットワーク
- 603 専門別ローカルエリアネットワーク
- 604 認証・振分け装置
- 618 デフォルトアドレスサーバ
- 622 認証サーバ
- 623 アドレス振分スイッチ
- 624 サブアドレス付与サーバ

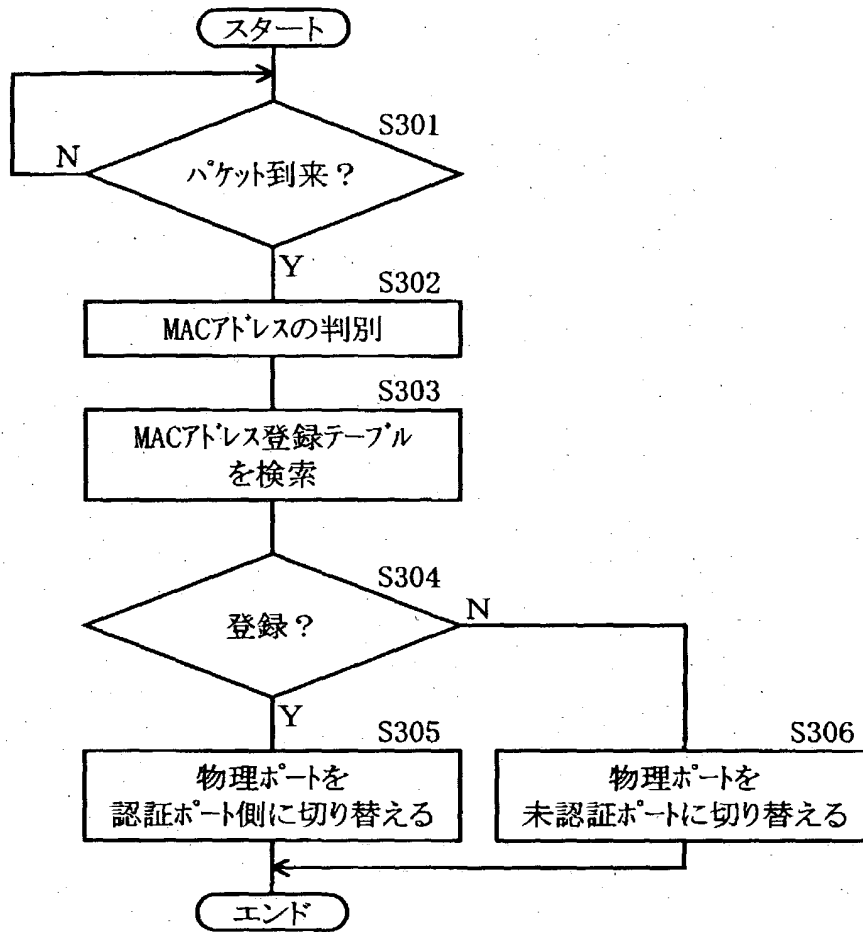
【書類名】

図面

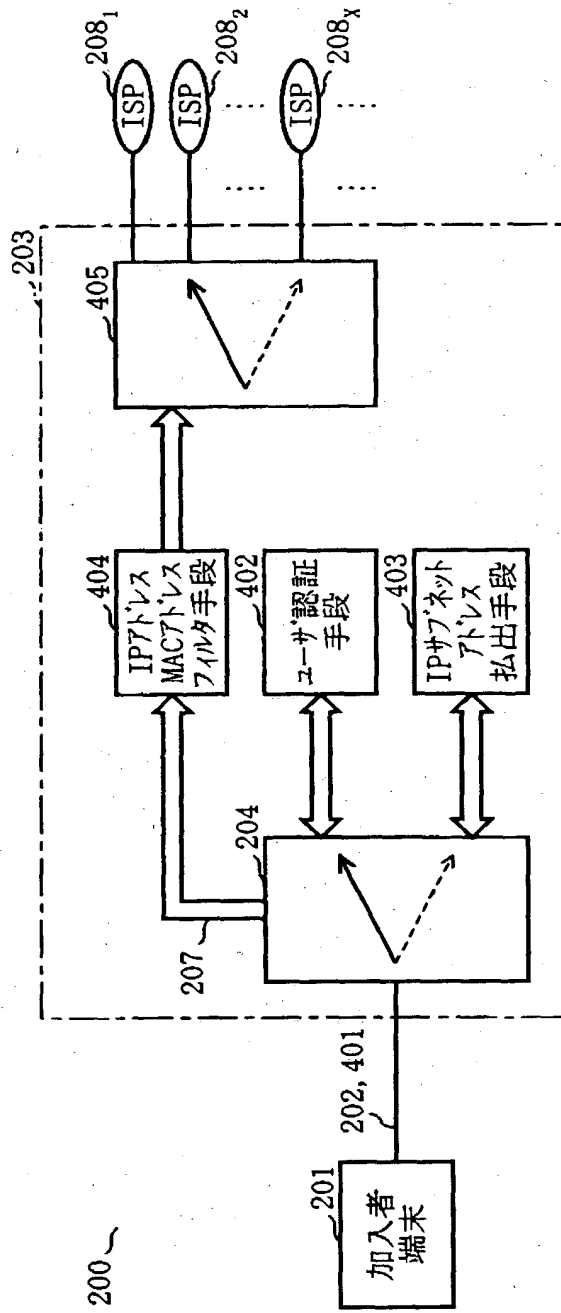
【図 1】



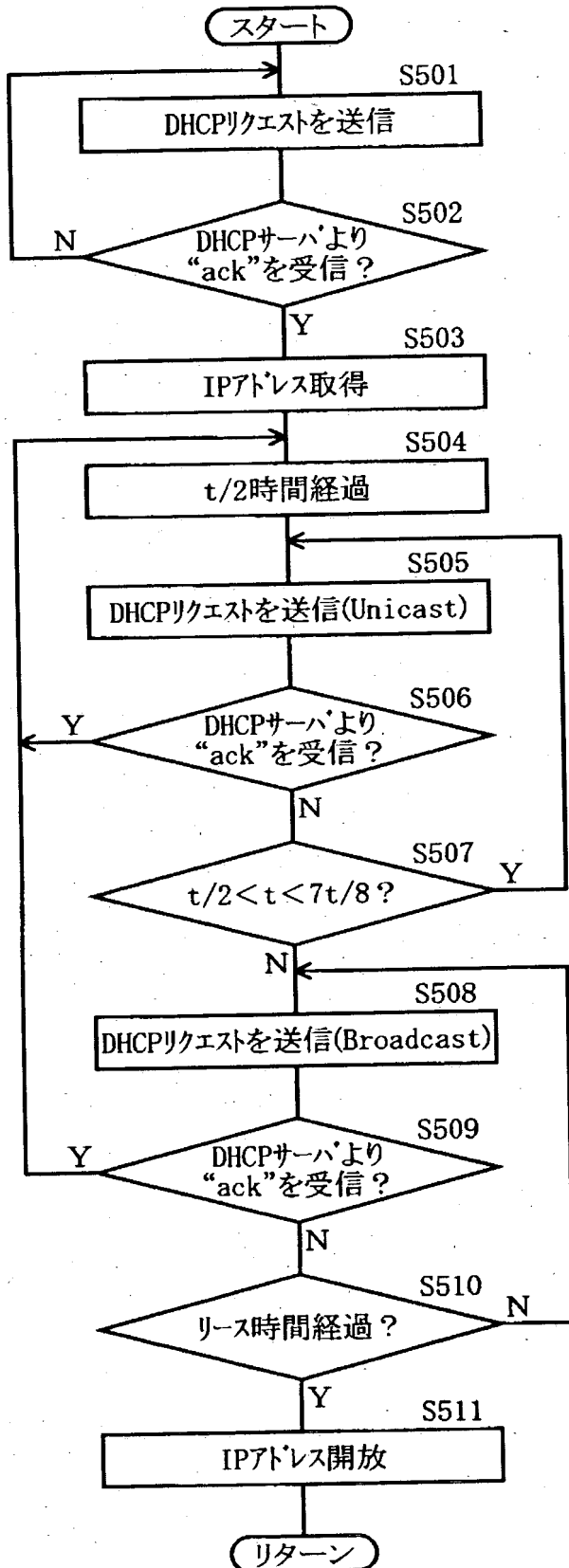
【図 2】



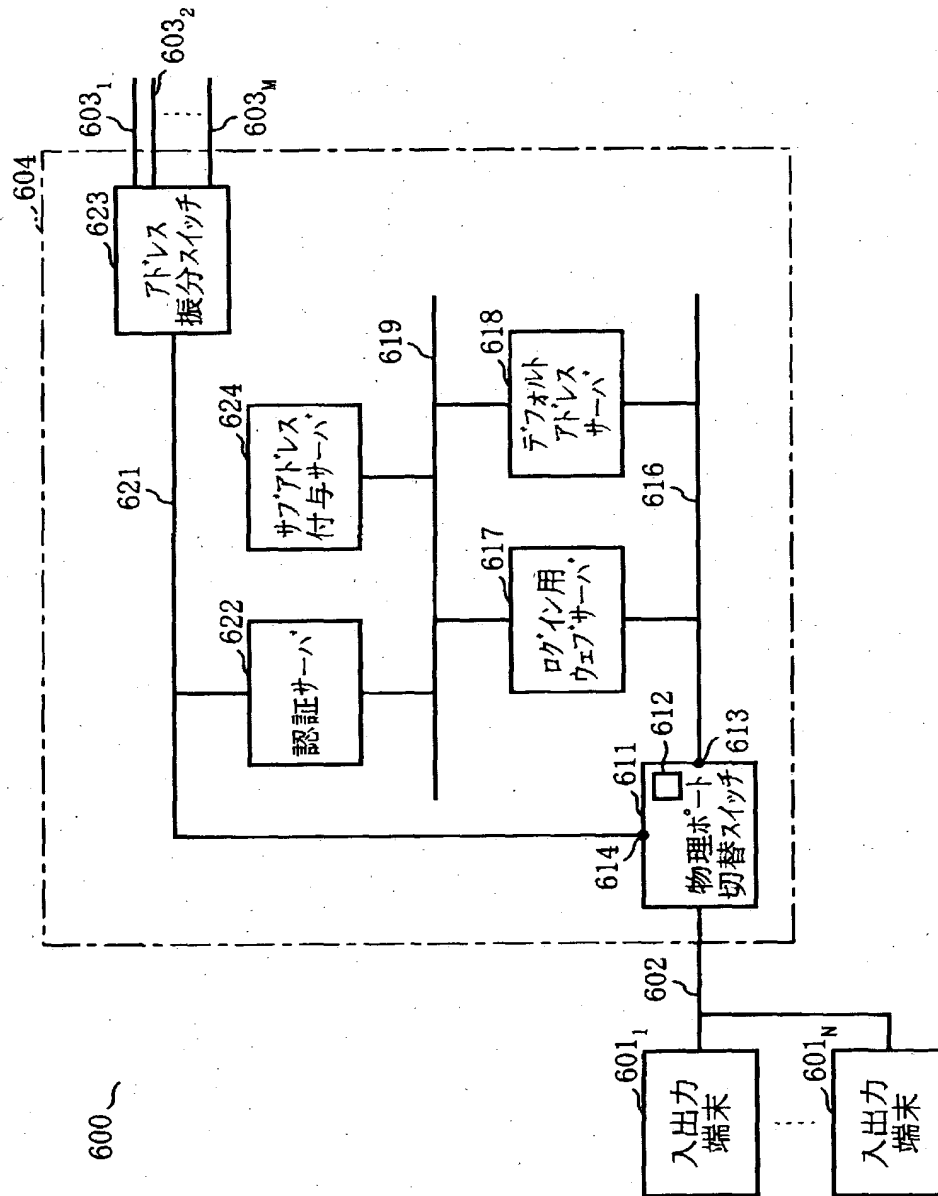
【図3】



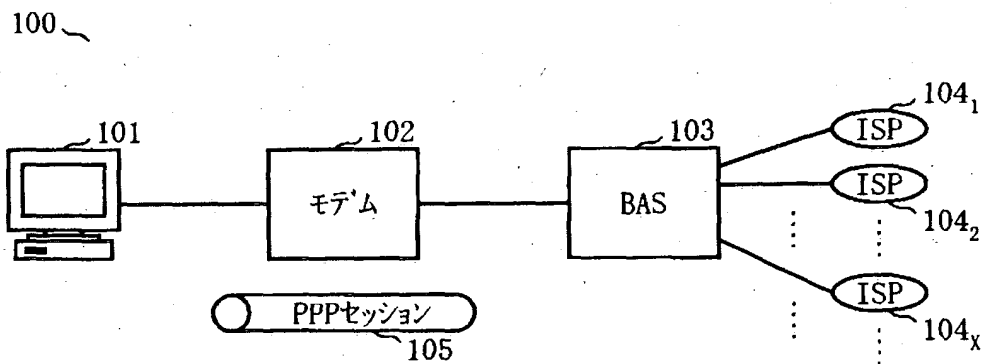
【図 4】



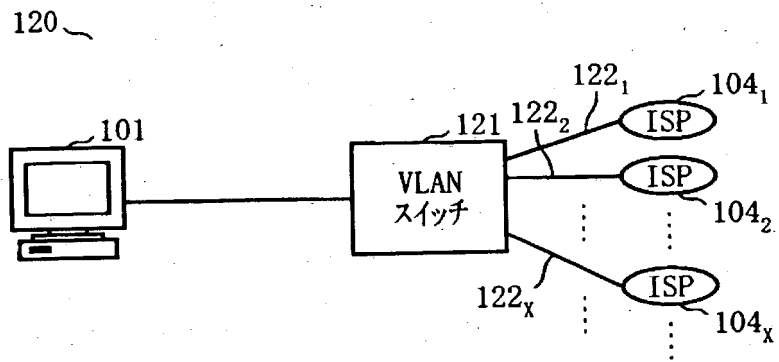
【図5】



【図6】



【図 7】



【書類名】 要約書

【要約】

【課題】 通信端末がローカルエリアネットワーク（LAN）を介して自在に通信ネットや所望のLANに数の制約なく接続することのできるユーザ認証システムおよびユーザ認証方法を得る。

【解決手段】 加入者端末201はLAN202およびネットワークサービスプロバイダ203内のIPサブネット振分スイッチ209を介してインターネットサービスプロバイダ208に接続される構成となっている。物理ポート切替スイッチ204は未認証の packets 信号を入力すると臨時のIPアドレスを加入者端末201に与え、これを用いて認証処理を行わせる。認証が成功したら正規のIPアドレスが付与され、これを使用した packets 信号はIPサブネット振分スイッチ209によって目的のネットワークに振り分けられる。

【選択図】 図1

特2002-200920

認定・付加情報

特許出願の番号	特願2002-200920
受付番号	50201008425
書類名	特許願
担当官	第八担当上席 0097
作成日	平成14年 7月11日

<認定情報・付加情報>

【提出日】 平成14年 7月10日

出 願 人 履 歴 情 報

識別番号

[000004237]

- | | |
|----------|---------------|
| 1. 変更年月日 | 1990年 8月29日 |
| [変更理由] | 新規登録 |
| 住 所 | 東京都港区芝五丁目7番1号 |
| 氏 名 | 日本電気株式会社 |